# Externe und applikationsinterne Autorisierung in OAuth2 Systemen

## Gliederung

1. Einleitung
2. Technische Grundlagen
   1. Erklärung grundlegender Begriffe
      1. Authentifizierung
      2. Autorisierung
      3. Integrität
      4. Authentizität
      5. Validierung
   2. OAuth2
      1. Rollen in OAuth2
         1. Resource Owner
         2. Resource Server
         3. Client
         4. Authorization Server
      2. Erhalt von Token
         1. Authorization Code Grant
         2. Refresh Token
   3. Rivest–Shamir–Adleman (RSA)
   4. JSON Web Token (JWT)
      1. JSON Web Key (JWK)
      2. JSON Web Signatur (JWS)
         1. RS256
   5. OpenID Connect
      1. ID Token
      2. Authorization Code Grant
   6. OAuth2 Endpunkte des Autorisationsservers
      1. Authorization Endpunkt
      2. Token Endpunkt
      3. JSON Web Key Set (JWKS) Endpunkt
   7. Zugriffskontrolle
      1. Role Based Access Control (RBAC)
      2. Attribute Based Access Control (ABAC)
3. Inhalt
   1. Problemstellung
      1. Einfluss von externer Autorisierung auf die Performanz
   2. Systemarchitektur
      1. Authorization Server Keycloak
      2. Postman
      3. Spring Boot
      4. Spring Security
         1. OAuth2 Resource Server
         2. Granted Authorities Mapper
         3. Access Decision Manager
      5. Open Policy Agent (OPA)
      6. Testsystem 1: Autorisierung in Ressourceserver
      7. Testsystem 2: Autorisierung entkoppelt von Ressourceserver mit Open Policy Agent (OPA)
   3. Tests und Testtools
      1. Metriken
         1. Latenz, Response Time, Datendurchsatz
         2. CPU-Auslastung, RAM-Belegung
      2. Erhalt eines Tokens durch „Authorization Code Grant“ mit Postman
      3. Apache JMeter
         1. Testplan Performanz
         2. Testplan Skalierbarkeit
         3. Testplan Last
      4. Windows Ressource Monitor
4. Experimente
   1. Auswertung
      1. Testplan Performanz
         1. Median, Mittelwert, Abweichung, Minimum, Maximum und Schwankung der Latenz
      2. Testplan Skalierbarkeit
         1. Berechnen einer Funktionsgleichung durch Approximation aus dem „Response Time Graph“
         2. Auswertung der approximierten Funktionen
      3. Testplan Last
         1. Median, Mittelwert, Abweichung, Minimum, Maximum und Schwankung der Latenz
         2. Datendurchsatz
      4. Windows Ressource Monitor
         1. CPU-Auslastung
         2. RAM-Belegung
5. Stand der Technik (Related Work) / Ausblick
   1. Neue Spezifikation für feinkörnige Autorisierung in OAuth2 in Arbeit - „OAuth 2.0 Rich Authorization Requests“
6. Zusammenfassung